Bachelor's Thesis (UAS)

Degree Program of Information Technology

2012

Lin Tong

The Design and Implementation of Company Network Security Architectures

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Information Technology | Internet Technology

Date | Number of pages

Instructor: Patric Granholm

Lin Tong

The Design and Implementation of Company Network Security Architectures

Nowadays, with the rapid development of internet technology and continuous expanding of networking scale, more and more facilities (such as governments, institutions and enterprises) enhance their dependency on networking to transmit and manage information more constantly. However, under the complex environment of information transmitting, information security is facing several risks. Upon such reality, networking security has become "the bottleneck" of popularizing internet.

The networking security issue combines not only technology but also strategy and management. Thus, a company's information security issue is a comprehensive process, and a systematic project.

This thesis mainly focuses on research and discussion about how to secure an enterprise network during designing and implementation. Meanwhile, the thesis discusses the essential aspects (such as firewalls, intrusion detection systems and Virtual Private Networks) involved during the procedure of securing network system and finding security solutions.

The thesis examines an enterprise as an example for designing network security architectures. When designing and implementing the security principles for an enterprise, both data protection and networking availability have to be considered as factors. The purpose of such an example is to reflect the key concepts and vulnerability of information security, then to offer and present the countermeasures to solve these problems from the aspect of networking security definition, characteristic structure and threat. By completing all the components entailed in the enterprise networking system accordingly, the goal of designing enterprise network is thus achieved. Finally, this thesis presents a case study of a company security architecture.

KEYWORDS:

(Enterprise network, Information Security, Network Security Architectures)

FOREWORD

This thesis introduces technologies about securing a network for an enterprise. The case is based on my work placement in Wuhan Fiberhome. I would like to thank my supervisor Mr Patric Granholm and my work placement project manager Xiao Hui.

2012 Turku Finland

Lin Tong

CONTENTS

LIST OF FIGURES

ACRONYMS, ABBREVIATIONS AND SYMBOLS

IPv4	Internet Protocol version 4
LAN	Local Area Network
WAN	Wide Area Network
VPN	Virtual Private Network
VLAN	Virtual Local Area Network
DoS	Denial of Service
DDoS	Distributed Denial of Service.

1 Background

The innovation of Internet technology has permeated people's life in many aspects. The invention of internet has popularized various fields, including business. An enterprise with a well-managed network will greatly increase its working efficiency. Unfortunately, network technology is a "double-edge sword", along with its strength there comes potential threats. To prevent different threats, and guarantee the company's business running in a safe environment, a security system is urgently required.

IPv4 (Internet Protocol version 4) protocol has more than thirty years history, and is still the most widely deployed internet layer protocol. Although there have been many improvements on IPv4, it has yet exposed many weakness. With the long-term development of internet technology, hackers have also developed their ability to take advantage of the protocol weaknesses, and use them for malicious purposes.

Although IPv6 will replace IPv4 in the future, most enterprises in China are still using IPv4 protocols; therefore this thesis mainly focuses on protocols security based on IPv4.

2 Analysis on enterprise network security

2.1 Enterprise network security

Network security involves protocols, technologies, devices, tools and techniques to secure data and mitigate threats [1]; it is an indispensable part of networking. Once an enterprise network has been breached, it will bring about the following consequences:

(1) Loss of business data,

(2) Disruption of e-commerce,

(3) Invasion of privacy, and compromise of the integrity of information.

2.2 The main goal of a secure enterprise network

Maintaining a secure network ensures the safety of network users and protects commercial interests [1]. The main goal of secure enterprise network is nondisclosure of information while storing and transmitting. Thus the following aspects will be considered while securing the enterprise network:

(1) Confidentiality: Ensuring the content of information will not be exposed to unauthorized users.

(2) Integrity: Data modification cannot be applied by unauthorized users.

(3) Availability: The authorized users can access data when necessary.

(4) Controllability: The information flow can be controlled by the administrator.

(5) Reviewability: Monitored the network flow and record unusual behavior.

2.3 The peculiarities of an enterprise network

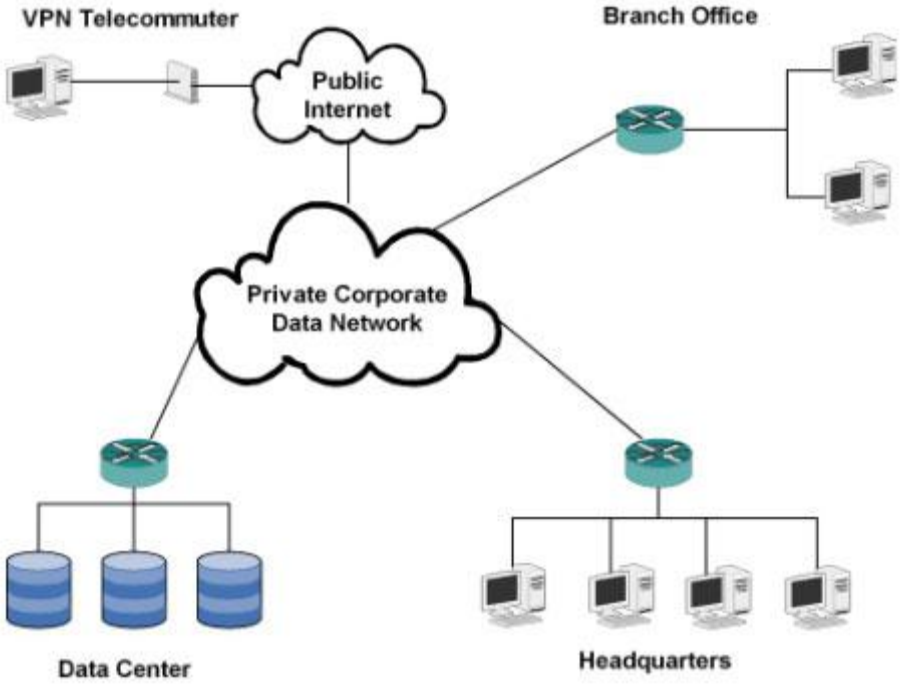

Figure 2.1 A simplified enterprise network

Every enterprise has its own demand for network, and the structure may vary. For example, a small size company contains only ten computers in one room; a big corporation may own thousands of computers in a building.

Although the difference in scale of enterprise is rather huge, the structure is similar and listed below as every network comprises of the following elements:

Internet

This refers to the Wide Area Network. Employees in enterprise can access the outside network.

Private network

This refers to the Local Area Network .Employees can share information and resources within the enterprise.

VPN

This refers to the Virtual Private Network. Employees can have remote access to the private network through public internet.

VLANs

*They r*efer to the Virtual Local Area Network. An enterprise will divide VLANs for departments located in different area.

Servers

They provide service to customers.

3 Possible threats to an enterprise network

Before establishing the defense system for an enterprise network, it is necessary to know what kinds of threats an enterprise is facing, and provide solutions accordingly.

3.1 Inside threats--LAN security

Either intentional or accidental, inside threats can cause greater damage than external network threats. The reason is that within the private network, users always have higher priority to directly access the enterprise data.

3.2 Viruses, Worms, and Trojan horses

Most employees in an enterprise are the clients or end-device users, and the primary threats for such group come from virus, worms and Trojan horses. Although they are just small executable programs, these tiny pieces of code can cause inestimable amount of damage. Virus, worms and Trojan horses behaving as follows:

- Viruses normally attach to a program (not virus itself) and are executed on victim computer for illegal purpose.
- Worms infect a computer by installing copies of itself in memory, thereby infecting other hosts.
- Trojan horses always fake as a harmless application. Once a Trojan horse is downloaded and opened, it provides hackers with remote access to a target computer and causes important information leakage, such as passwords.

Viruses, worms, and Trojan Horses are performed as end-users' threats [1].

3.3 Different attacks

There are many different types of network attacks and they can be categorized as below:

Information-gathering Attacks

Information-gathering attacks are also called reconnaissance attacks. The purpose of information-gathering attack is to discover target computer without authorization. These kinds of attack often employ software such as Sniffers, which can be easily found on the Internet.

The tools used for information-gathering attack are:

- Packet sniffers
- Ping sweeps
- Port scanners
- Internet information queries

An information-gathering attack will not take control of the target directly. Instead, it will collect information from the target for future intrusion [2].

Access Attacks

Access attacks exploit known vulnerabilities in authentication services, FTP services, and web services to gain entry to web accounts, confidential databases, and other sensitive information [1]. Access attacks are performed in the following ways:

- Password attack: This aims to guess the passwords of a system.
- Trust exploitation: This grants privileges of a system in an unauthorized way.
- Port redirection: This redirects traffic from a certain port to another.
- Man-in-the-middle attack: This monitoring traffic between users in order to read or modify the date passing through.
- Buffer overflow – A program overloads data to memory than its own intention, then causes overwriting of valid data or executes malicious code.

The purposes of launching an access attack are: retrieving data, gaining access, and escalating access privileges [2].

DoS/DDoS Attacks

DoS refer to Denial of Service and DDoS refer to Distributed Denial of Service. These attack methods aim to slow or crash down the target by sending a large amount of requests so that the target can hardly handle such unexpected condition and fails to process valid requests due to limited hardware resource. The target can be a server, a network host, or an application [3].

DoS/DDoS attacks are the most threatening method than other attacks for two reasons:

1. Once a DoS attack occurs, its activity will impact enterprise business and cause great loss.

2. A DoS/DDoS attack requires less knowledge and is easily generated.

The intention of DDoS attack is similar to DoS attack, except that DDoS starts its attack from multiple sources which are organized.

4 Firewall Technology

4.1 Firewall concepts

In the older times, when humans lived in wooden houses, people piled up stones around their house to prevent fire accidents, this is, the so-called firewall. In the late 1980s, when internet technology started to be widely used for global connections, the term firewall referred to a new technology which had the same function as that of a physical firewall. The following paragraphs explain the firewall concepts and functions from different aspects: [4]

(1) A firewall is an access control technology, which can set barriers between an organization's network and an outside network in order to prevent illegal access to the organization's information resources. In another way, a firewall is a threshold that can control the in/out communications in both ways.

(2) A firewall is a device or a set of devices deployed on the edge of two networks. Such devices have the following properties:

a) Only allow the local security policy authorized message going through.

b) Both way communications must travel through firewall.

c) A firewall itself will not affect the information content.

(3) A firewall is a combination of hardware or software which is located between a trusted and an untrusted network (such as an enterprise internal network and the Internet), and manage the connections between two networks by enforce unified security policy to protect data resources from illegal access or modification.

A firewall aims to protect an internal network from an external network intrusion. Typically it refers to enterprise network as internal network and the Internet as external network. However, a firewall not only applies to the Internet, but also applies to internal network between different branch departments, for example, the marketing and financial department.

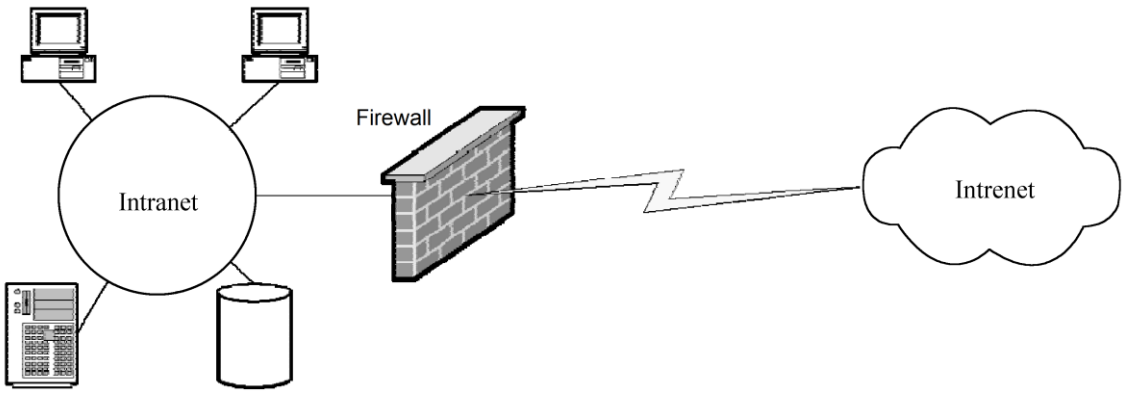

Figure 4.1 Firewall example

In Figure 4.1, a firewall is deployed between the Internet and Intranet. The firewall system decides which inside service can be accessed from the outside network and by whom and which outside service can visit from inside network. When implementing a firewall, all traffic flow must travel through the firewall for inspection. Firewalls permit the traffic matching the filter rules and block the mismatching one.

4.2 Firewall functions

A firewall is an access controlling system between networks, normally deployed at the access point on the edge of the internal and external network. A firewall is not only applied as software or hardware, but also as a part of access control policy. An access control policy is simply a corporate policy that states which type of access is allowed across an organization's network perimeters [2]. Without an access control policy, a firewall is a useless machine. Firewall executes security policy and control network access by the following methods [4]:

(1) Service control which ensures the access types of service. A firewall can filter packets based on IP address and TCP ports.

(2)Direction control which ensures the permitted service requests will not be blocked.

(3)Authorization control which requests authorization when users are trying to access a service.

(4)Behavior control which controls how to access a specific server.

4.3 Firewall categories

In terms of the concepts and functions, firewalls can be divided into the following categories below: [2]

- *Embedded firewalls*

  A firewall is embedded when firewall functions are integrated into a router or a switch. This type of firewall is known as a choke-point firewall as well. Embedded firewalls normally perform stateless inspection (only examine the source and destination address of an IP packet) of packets at the network layer only, resulting in faster performance but an increased vulnerability to malicious attacks.

- *Software firewalls*

  Software firewalls are divided into two different types. One is enterprise class which can perform routing functions for large networks, while the other is a Small Office, Home Office (SOHO) class which generally can provide the full range of firewall features. These kinds of firewalls are installed on server-based hardware and operating systems (like Windows).

- *Hardware firewalls*

  Hardware firewalls are known as appliance firewalls as well. They are intended to be turnkey systems which need no configuration or extensive installation before they start to provide firewall function services. Hardware firewalls , similarly to software firewalls, can be functional either on the enterprise or the Small office, Home Office (SOHO) markets.

- *Application firewalls*

  Application firewalls which on purpose, provide a sophisticated level of information filtering for data traveling at the layer 7 that is application layer, are normally implemented as additional components to existing software or hardware firewalls. These kinds of firewalls are becoming more and more specialized, because firewall functions increase in their capabilities, and filtering focuses increasingly on data of the upper layer.

4.4 Firewall structure

Packet filtering firewalls

A packet filtering firewall is often part of a firewall program for protecting a local network from intrusion on a router. It works at the transport layer of the seven layer model, is deployed on routers and act as a bottleneck between the internal network and the Internet. A packet filtering firewall inspects every packet passing through based on the previous defined security policy rules. [6]

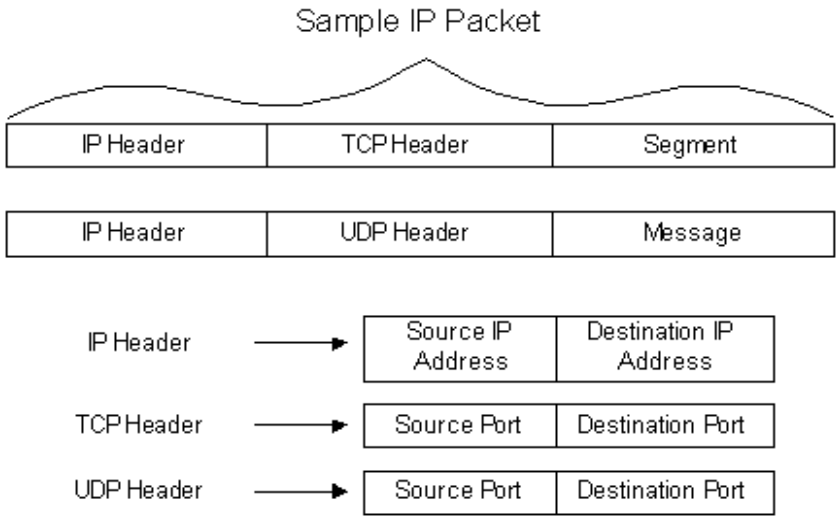

Figure 4.4 Sample IP Packet

According to the sample IP packets figure, packet filters inspect the following attributes of a packet:

- Source IP address
- Destination IP address
- TCP/UDP source port
- TCP/UDP destination port

There are two ways to perform a packet filtering operation:

- Accepting all packets except those which are specified as denied.

- Denied all packets except those which are specified as permitted.

Circuit Level Gateways

When an external user wishes to access information on a file server behind a firewall, the security policy from the network will not permit a direct connection between the external user and the file server because such action may leave the network vulnerable to attack. To solve this problem, two parties can create a “tunnel” between the two components, employing a method of encryption in the connection.

Application Gateways

Application gateways are also called proxies and are commonly used as firewall mechanisms. While remote access to other components of the network is not allowed, the inclusion of components in a demilitarized zone (DMZ, the area between two firewalls) would allow access to components which were needed by the external network users. Restricting the access to components via a DMZ, and through the use of a proxy server allows external users to perform functions on servers such as the WWW server or the DNS server. In this way, DMZ satisfies the external users’ requirement but will not disclose the architectural details of the LAN.

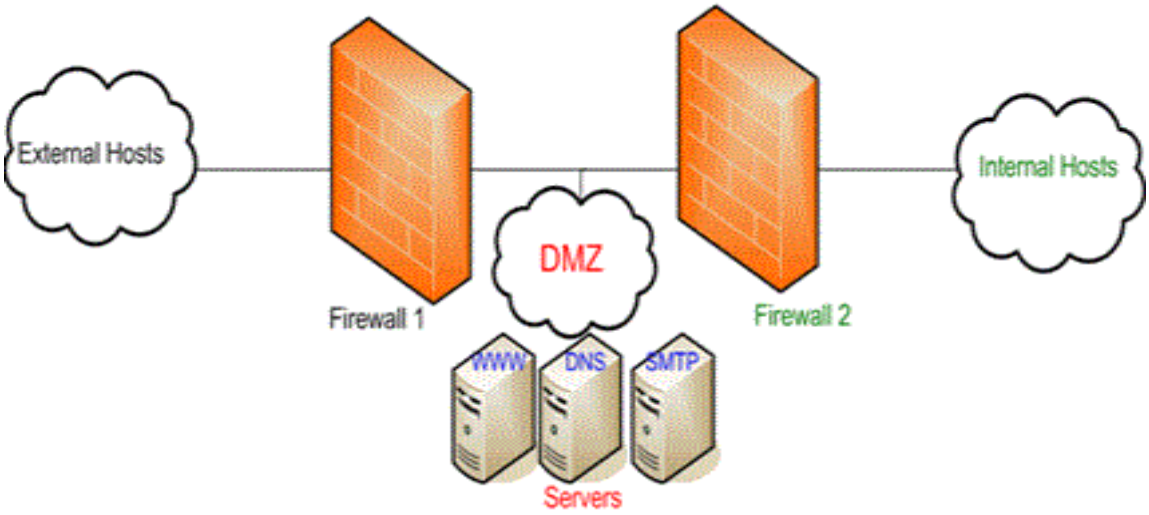

Figure 4.5 DMZ

5 Intrusion Prevention Systems

In traditional network security technology, most defense strategies are passive, for example, the access control list in a firewall. Based on the complexity of network, the passive strategy is insufficient. In order to convert the network defense from passive to active, the *P2DR* model is proposed.

P2DR stands for: *Policy, Protection, Detection and Response*. The model figure is shown below:

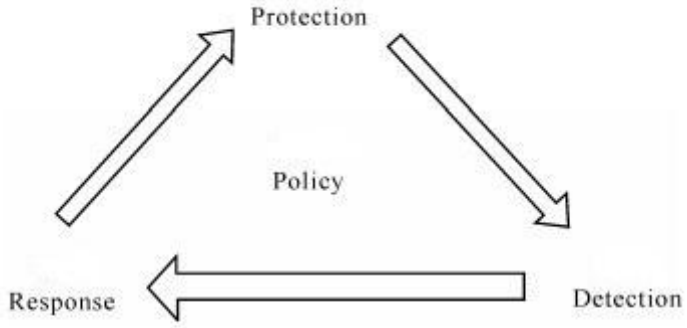

Figure 5 The P2DR model

The P2DR model works under security policy and guidance, by taking advantage of defense tools (such as firewall, identification system and encryption) and detection tools(such as vulnerability assessment and intrusion detection system), to evaluate a system's safety status. Thereby it alerts the network administrator to set the defense system to "most secured" and "lowest risk" condition. [8]

5.1 Intrusion Detection Technology

IDS (Intrusion Detection System) are an active network security technology to protect a network from illegal attacks. IDS collects and analysis information from the computer system or network, detects any behavior of security policy violation or sign of attack, intentions of breaking information's integrity, confidentiality and availability, and response accordingly.

5.2 Intrusion Detection Compositions

In general, IDS consists of four modules, they are:

Event generators

Event generators are in charge of collecting original data. They trace data flow and log file, then convert them into “events” and submit them to event analyzers and event database.

Event analyzers

Event analyzers analyze the event information from generators, make judgments if the events are intrusions or unusual phenomena and then report to the administrator.

Event database

An event database is a storage space for temporary and permanent data. An event database can be either complex database, or simply text file.

Response units

Response units are the heart of IDS. When intrusion behavior is detected, the response units react immediately. The reaction includes disconnect, change file authority and alarm.

5.3 Functions of Intrusion Detection

The functions of IDS are: detecting alarm and expelling intrusion behavior; minimizing loss during intrusion; gathering information about the intrusion event, inserting it into the database to improve the ability of defense. The main functions of IDS are to:

1. Monitor, analysis the activities of users and system.
2. Detect intrusion intention.
3. Record, alarm and response.

IDSs are not a preventive measure. They will not stop intruders breaking into a system. Neither will they prevent internal damage to a system. They are a detection system, thus implying that abuse of a system is reported as and when it happens [7].

5.4 Types of IDSs

Just like a firewall, different types of intrusion detection systems exist. There are several places throughout a system to place an IDS including on switches, routers, or within programs. Depending on position of the deployment within a network, IDSs can categorize as into *network based*, *host based* or *application based*. [7]

Network-based IDS

This type of IDS sniffs the traffic on the network by capturing packets of data(often IP data) and using them in the analysis. Data capture is performed at the network switch level, so providing detection for traffic going in and out of multiple hosts. Such a deployment method is a good solution for large scale networks because it simplifies the conversion of many hosts in one detection system.

Host-based IDS

Host-based IDS use a bottom system based on a per host distribution. This method analyzes the traffic and detects any disruption with greater accuracy. Additionally, logs based on the host machine record the outcome of an attack, which can assist in the development of various countermeasures.

Application- based IDS

The application-based IDS is a subset of host based system. This type of IDS is installed on a host computer and analyzes the behavior of running applications. All unauthorized usage of applications will generate information to application logs for detection [7].

5.5 Intrusion Prevention System (IPS)

Both the Intrusion Detection System and the Intrusion Prevention System work as sensors within the network layer.

IPS (Intrusion Prevention System) builds upon IDS technology. Intrusion Detection Systems was implemented to passively monitor the traffic on a network. An IDS-enabled device copies the traffic stream, and analyzes the monitored traffic rather than the actual forwarded packets. It compares the captured traffic stream with known malicious signatures in an offline manner similar to software that checks for viruses. The disadvantage of IDS is that IDS can only monitor the traffic and respond to the network administrator. Unlike IDS, an IPS device is implemented in inline mode. This means that all income and outgoing traffic must flow through it for processing. An IPS does not allow packets to enter the trusted side of the network without first being analyzed. It can detect and immediately address a network problem as required.

IPS workflow:

1. An attack is launched on a network that has a sensor deployed in IPS mode(inline mode).

2. The IPS sensor analyzes the packets as they enter the IPS sensor interface. The IPS sensor matches the malicious traffic to a signature and the attack is stopped immediately.

3. The IPS sensor can send an alarm to a management console for logging and other management purposes.

4. Traffic in violation of policy can be dropped by an IPS sensor [1].

Similar to IDS, IPS also has network-based implementations and host-based implementations.

Network-based IPS implementations

Network-based IPS implementations analyze network-wide activity looking for malicious activity. Network devices such as ISR routers, ASA firewall appliances,

Catalyst 6500 network modules, or dedicated IPS appliances are configured to monitor known signatures. They can also detect abnormal traffic patterns [9].

Host-based IPS implementations

Host-based implementations are installed on individual computers using host intrusion prevention system (HIPS) software such as Cisco Security Agent (CSA). HIPS audits host log files, host file systems, and resources. A simple form of HIPS enables system logging and log analysis on the host, which is an extremely labor-intensive approach. CSA software helps manage HIPS and proactively secures hosts. A significant advantage of HIPS is that it can monitor operating system processes and protect critical system resources, including files that may exist only on that specific host. It combines behavioral analysis and signature filters with the best features of anti-virus software, network firewalls, and application firewalls in one package [9].

A network must be able to instantly recognize and mitigate worm and virus threats. Intrusion prevention is required throughout the entire network to detect and stop an attack at every inbound and outbound point. It is better to implement a solution that detects and immediately addresses a network problem as required.

6 VPN Technology

VPN (Virtual Private Network) takes advantage of a public network to transmit messages to form logical private networks. The purpose of VPN is to contrast public Internet. As we know, the Internet is public and can be accessed without authorization. Therefore, it is trustless. Virtual private network technology is implemented by organizations to establish end-to-end private network connections over third-part networks (such as the Internet or an external network). The connection enables remote users to access internal network resources which are private and secured. In general, VPN aims to provide logical virtual subnets for enterprises private networks. Sometimes enterprises have branch offices in different locations. The sharing of data resources between branch departments has become an important issues. Enterprise communications contain lots of private information and therefore should be transmit secretly. A typical VPN system consists of four parts:

VPN server

It responds to a VPN client connection request.

VPN clients

Clients are end-devices, such as computers or routers.

VPN tunnel

It encapsulates a data transmission channel.

VPN connection

Traffic flow must be encrypted during transmitting.

6.1 VPN categories

VPNs implement logical network technology on physical network layer, thus it is an independent network.

VPNs can be classified into three categories according its functions:

(1) VPDN: Virtual Private Dial Network

(2) Intranet VPN

(3) Extranet VPN

6.2 Basic types of VPN networks

In Figure 6.2, the white cloud represents public Internet, the connections of two regional offices through public internet is using site-to-site VPN, and remote users are using remote-access VPN. Site-to-site VPN and remote-access VPN are the basic types of virtual private network [9]:

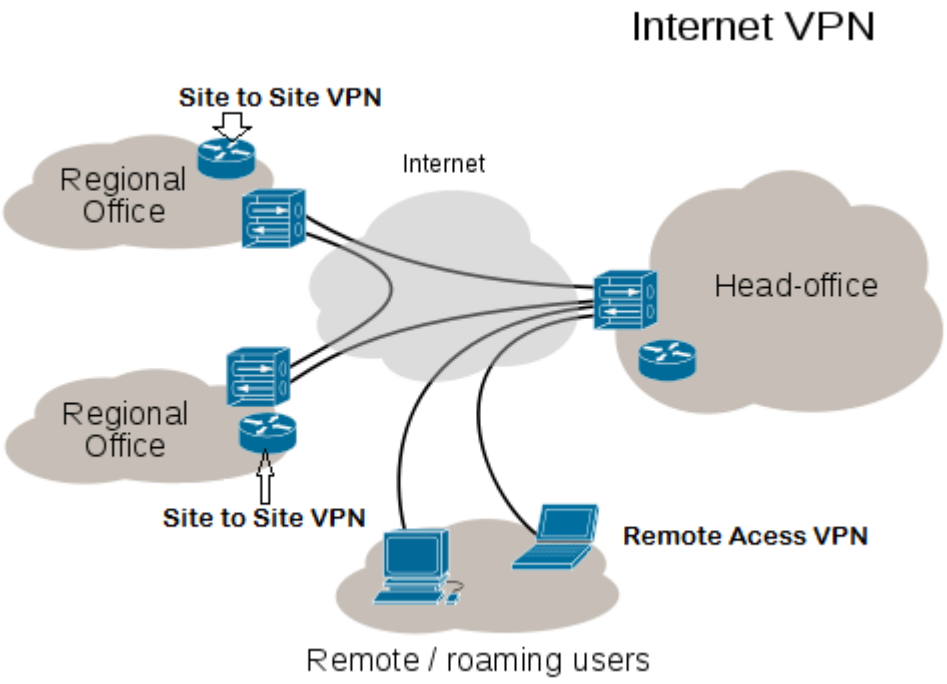

Figure 6.2 VPN system structure

(1)Site-to-site VPN

A site-to-site VPN is created when connection devices on both sides of the VPN connection are aware of the VPN configuration in advance. The VPN remains static, and internal hosts have no knowledge that a VPN exists. Frame Relay, ATM, GRE, and MPLS VPNs are examples of site-to-site VPNs.

(2)Remote-access

A remote-access VPN is created when VPN information is not statically set up, but instead allows for dynamically changing information and can be enabled and disabled. Let us consider a telecommuter who needs VPN access to corporate data over the

Internet. The telecommuter does not necessarily have the VPN connection set up at all times. The telecommuter's PC is responsible for establishing the VPN. The information required to establish the VPN connection, such as the IP address of the telecommuter, changes dynamically depending on the location of the telecommuter.

Although VPN technology provides network communication for enterprises, VPN cannot guarantee information security while traversing the tunnel because VPN tunnels are founded based on public network. For this reason, VPN technology is always applied with modern cryptographic methods, in order to secure private network connections.

6.2 IPSec framework

The IP Security (IPsec) protocol provides a framework for configuring secure VPNs and is commonly deployed over the Internet to connect branch offices, remote employees, and business partners. It is a reliable way to maintain communication privacy while streamlining operations, reducing costs, and allowing flexible network administration.[1]

IPSec is neither a specific encryption algorithm nor an authentication algorithm, nor does it define an encryption algorithm or and authentication algorithm in its data structure. IPsec provides unified data framework for encryption and authentication algorithms, in a way to standardize and improve data security policy. Meanwhile, a variety of encryption algorithm can applied to the IPSec framework during network data transmitting.

IPSec protocols include two parts: security protocol and key agreement. Security protocol defines the methods in communication; key agreement defines parameter for security agreement and identification.

6.3 IPSec security protocol

A security protocol that guarantees combinations of authentication, integrity, access control, and confidentiality, will provide cryptographic security services in the network layer.[11]

6.3.1 Confidentiality - IPsec ensures confidentiality by using encryption. Two of the main encryption algorithms are:

(1) Data Encryption Standard (DES): This is a symmetric encryption algorithm used for both encryption and decryption which encrypts data in 64-bit block mode with an encryption key.

(2) Triple Data Encryption Standard (3DES): This is a symmetric encryption algorithm which increases the DES effective key length to utilize the same formula with different keys several times in a row.

6.3.2 Integrity

IPsec ensures that data arrive unchanged at the destination using a hash algorithm such as MD5 or SHA. Two of main relevant algorithms are:

(1) Message-Digest Algorithm (MD5): This algorithm is used in a variety of internet applications. It uses a one-way hashing function which is easy to compute hash and unfeasible to compute data given a hash. It also produces a 128-bit hash from a complex sequence of simple binary operations.

(2) Secure Hash Algorithm (SHA): This algorithm takes an input message of less than 2^64 bits and produces a 160-bit message digest. The algorithm is slightly slower than MD5.

SHA-1 is a revision that corrected an unpublished flaw in the original SHA.SHA-224, SHA-256, SHA-384, and SHA-512 are newer and more secure versions of SHA and are collectively known as SHA-2.

6.3.3 Authentication

IPsec uses Internet Key Exchange (IKE) to authenticate users and devices that can carry out communication independently. IKE uses several types of authentication, including username and password, one-time password, biometrics, pre-shared keys (PSKs), and digital certificates. The following parts introduce two of main authenticated algorithms and two security protocols.

.

(1) Pre-shared keys (PSK) are combined with other information to form the authentication key which requires each peer to authenticate its opposite peer before the tunnel is considered secure. Although it is easy to configure manually, it is not scalable, because each IPsec peer must be configured with the PSK of every other peer.

(2) The Ron Rivest, Adi Shamir and Leonard Adleman (RSA) algorithm is based on the presumed difficulty of factoring large integers. RSA signature is the technology exchanging the digital certificates to authenticate the peer.

6.3.4 Encapsulating Security Payload

Encapsulating Security Payload (ESP) which is IP 50 can provide confidentiality authentication and integrity. At a minimum, one form of encryption and authentication must be selected.

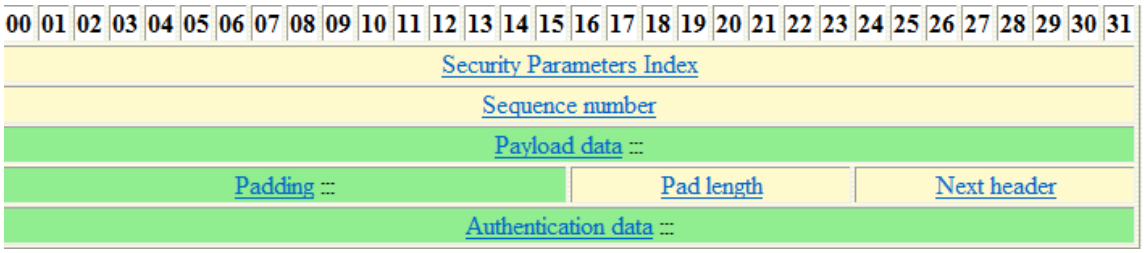

Figure 6.3.1ESP framework

6.3.5 Authentication Header

Authentication Header (AH) which is IP 51 can provide data authentication and integrity for IP packets. AH does not provide data encryption of packets.

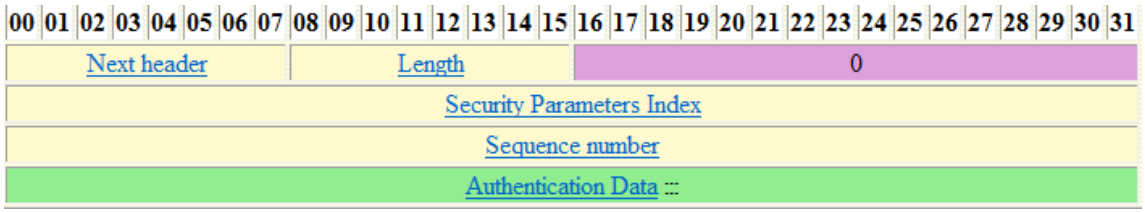

Figure 6.3.2 AH framework

7 Designing and implementing enterprise security architecture

The author took part in establishing a network security system during work placement in Wuhan Fiberhome. The main objective of the project was to establish a firewall for the sub company which is in a different location. The main work for author was configuring the routers and enabled all the services according the project book under the guidance of my project manager.

7.1 Introduction of project

Referring to the Figure 7, a firewall is deployed at the edge of the intranet. In this project, the administrator chose an embedded firewall, and set access control rules accordingly. DMZ can provide various services. This sub company communicates with the main company through site-to-site VPN secured connection.

7.2 Topology of an enterprise network

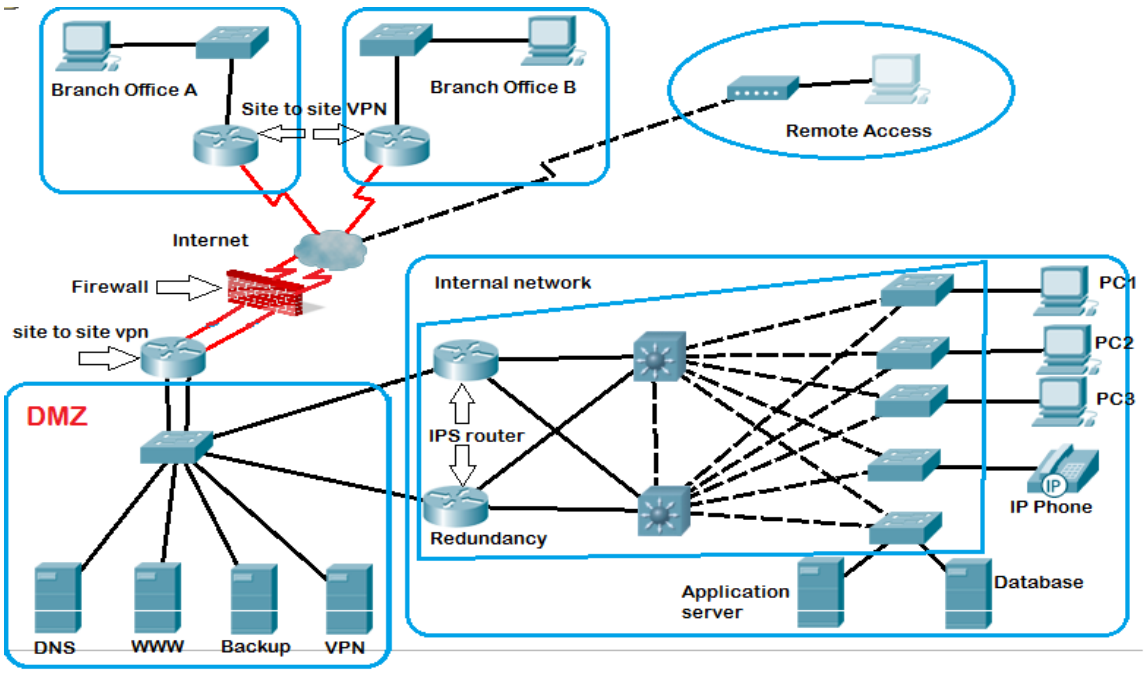

Figure 7 An enterprise network topology

In Figure 7, this topology graphic is a screen shot from a packet tracer model, which is simulated to the project book. The two branch offices represent the Production department and Purchasing department which are few hundred meters away from the sub company. In this sub company, two layer 3 switches are set to trunk mode aim to establish communication between layer 2 switches. PC1, PC2 and PC3 represent to three offices.

7.2 Defining an Access Control Policy

Before a firewall configuration, we need to analyse the firewall system and define an access control policy. An access control policy is simply a corporate policy that states which type of access is allowed across an organization's network perimeters: what types of internet traffic are required to fulfil business functions; which types of services should be permitted to be accessed and the remaining request should be denied.

An access control policy can also apply to different areas within an internal network.

An access control policy simply defines the directions of data flow to and from different parts of the network. It also specifies what type of traffic is acceptable, assuming that all other data types will be blocked. When defining an access control policy, we can use a number of parameters to describe traffic flow [5].

7.3 Firewall selection

Various companies produce all kinds of firewalls with different functions. Their cost is based on the firewall's capability. The price increases when a firewall has a fast performance or stronger defence ability. Before purchasing a firewall, the network manager should evaluate the network environment within the enterprise, and choose a firewall with proper functions and price. In this case, the H3F100A router is chosen because of its multi-functions and proper price.

7.4 Firewall deployment

A firewall builds up the first defense line for an enterprise local area network. In the topology diagram, the firewall is located in the access point of the entire internal network. An enterprise local area network normally contains a couple of application servers such as a WWW server, a VPN server and a DNS server. These servers can be visited by both internal network and external network users. Thus, different access control policies are applied over servers and the internal network.

7.5 Configuration sample

In the figuration sample, the enterprise uses the H3F100A router which is a product of Huawei Company. The H3F100A router is a multi-functional router which integrates all functions of routing, firewall defence, IPS detection and VPN.

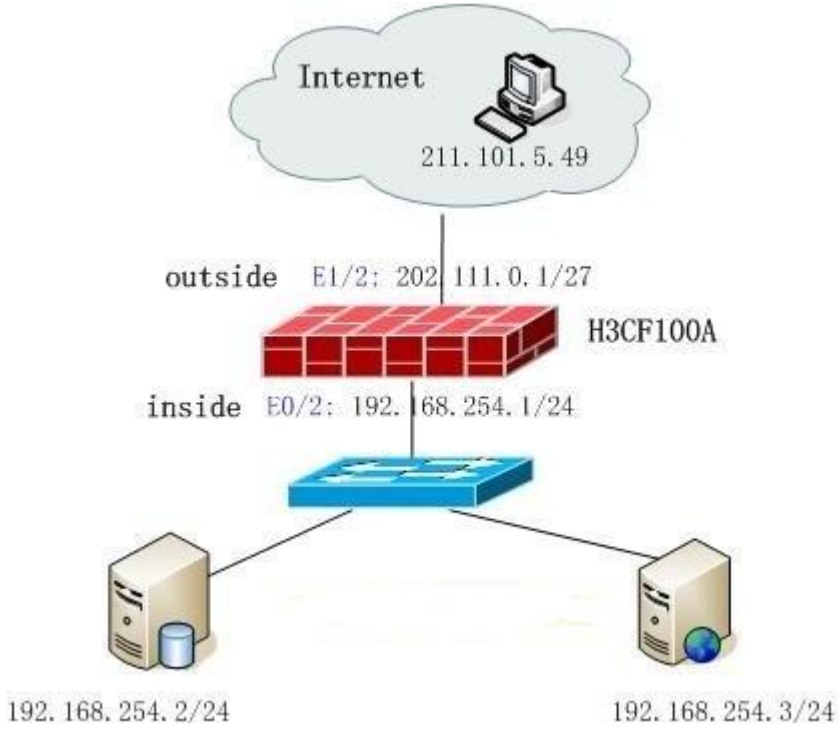

Figure 7.5 Topology of configuration sample

Configuration requirement

1) Firewall Ethernet port 2 is the trust area and its IP address is 192.168.254.1/29.

2) Firewall Ethernet port 1 is the untrusted area and its IP address is 202.111.0.1/27.

3) Internal network servers use static NAT to translate private IP addresses to public internet. The server with IP address 192.168.254.2/24 is mapping to 202.111.0.2/27 and the server with IP address 192.168.254.3/24 is mapping to 202.111.0.3/27.

4) The internal network server can access external network without limitation. The external network server can only access the internal network with the public address of 211.101.5.49, which is mapping to 192.168.254.2:1433 and 192.168.254.3:80.

Switches Security

The firewall, VPN and IPS can detect and prevent intrusion from the external network but they cannot do anything if an intentional intrusion breaks in the inside network. One prevention measure is to secure the switch port, and any changes without the administrator's permission will shut the switch ports down immediately.

Enabling VPN on Firewall

As introduced before, the H3F100A router also has the VPN function. After configuring the firewall function, the following step is to enable the client site VPN. The command for enabling VPN on firewall is described in the Appendix.

More details can be found in the Appendix.

8. Disaster prevention and Recovery

Disaster prevention means implementing precautionary measures that protect the network operation from any unexpected interruption, whether intentional or unintentional. All the previous parts of this thesis mainly describe intentional attacks and defense measures. But unexpected facts also have to be taken into consideration when securing an enterprise network.

8.1 Redundancy

From Figure 6, both DMZ and internal network use more switches than they actually need. The switches status may go down due to some uncertain reasons (for example, power supply disconnection). Once a switch goes down, the entire internal network stops operating. By implementing redundancy, the switches' convergence function will maintain the network's normal working condition.

8.2 Hardware protection

The hardware protection implements the following policies:

1) The physical condition of all devices, including host computers, printers, firewall, routers and switches. It ensures those devices are running under a proper electromagnetic environment.
2) Keeping the cables and devices in secured positions, avoiding incidental damage.
3) The operations room is accessed by authorized staff only.

8.3 Backup and recovery

As a network administrator, backup hardware' configuration and server' data is one of the important routines. When the hardware breaks down, the administrator can recover the failed system as soon as possible.

9. Conclusion

Network security guaranteeing the integrity, confidentiality and authentication of the enterprise, is the primary factor of the network structure. Threats should be considered not only externally intentional hackers but also internal operation incidents. Therefore, even the non-It support personnel should be educated about network security. Fortunately, backup recovering responds quickly to control infected devices. Networking security is not a one-step procedure but the strategy to handle the problems of known threats as well as to mitigate the effects of an unknown disaster. With the technology advancing fast, it is necessary to keep track of the development of the network security, which is a lasting topic of lasting importance.

REFERENCES

[1] Viruses, Worms and Trojan Horses [www-document]. Accessed: 16.05.2012 Available at:

http://ethics.csc.ncsu.edu/abuse/wvt/

[2] Ranum M.J. 2005. Internet Attacks. Boston, MA, USA: Addison-Wesley Longman Publishing Co, Inc.

[3] DsS/DDoS attack [www-document]. Accessed: 12.05.2012. Available at:

http://www.cert.org/tech_tips/denial_of_service.html

[4] Xu Guoai. 2004. Network security. Beijing, China: Beijing University of Posts and Telecommunications Press.

[5] Brenton C. & Hunt C. 2003. Mastering Network Security. SYBEX Inc. 1151 Marina Village Parkway, Alameda.

[6] Packet filtering firewall [www-document] Accessed: 17.05.2012. Available at:

http://securityworld.worldiswelcome.com/packet-filtering-firewall-an-introduction

[7] Smith J.G.& Aickelin U. 2005. Firewalls, Intrusion Detection Systems and Anti-Virus Scanners. Computer Science Technical Report No. NOTTCS-TR-2005-.

[8] Feng Yanfei & Du Jiang. 2009. Research of Policy Based on P2DR model. Chongqing, China: Chongqing University of Posts and Telecommunications, Department of Computer Science.

[9] VPN types [www-document]. Accessed: 19.06.2012. Available at:

http://www.cisco.com/web/learning/netacad/index.html

[10] IPSec protocols [www-document]. Accessed: 19.06.2012. Available at:

http://en.wikipedia.org/wiki/IPsec

[11] IP Security Protocol (IPSec) [www-document]. Accessed: 19.06.2012. Available at:

http://www.chineselinuxuniversity.net/courses/netsec/guides/4306.shtml

APPENDIX 1

FIREWALL CONFIGURATION SCRIPT

<H3CF100A>dis cur
#
sysname H3CF100A
#
super password level 3 cipher 6aQ>Q57-$.I)0;4:\(I41!!!
#
firewall packet-filter enable
firewall packet-filter default permit
#
insulate
#
nat static inside ip 192.168.254.2 global ip 202.111.0.2
nat static inside ip 192.168.254.3 global ip 202.111.0.3
#
firewall statistic system enable
#
radius scheme system
server-type extended
#
domain system
#
local-user net1980
password cipher ######
service-type telnet
level 2
#
aspf-policy 1
detect h323
detect sqlnet
detect rtsp
detect http
detect smtp

detect ftp
detect tcp
detect udp
#
object address 192.168.254.2/32 192.168.254.2 255.255.255.255
object address 192.168.254.3/32 192.168.254.3 255.255.255.255
#
acl number 3001
description out-inside
rule 1 permit tcp source 211.101.5.49 0 destination 192.168.254.2 0 destination-port eq 1433
rule 2 permit tcp source 211.101.5.49 0 destination 192.168.254.3 0 destination-port eq www
rule 1000 deny ip
acl number 3002
description inside-to-outside
rule 1 permit ip source 192.168.254.2 0
rule 2 permit ip source 192.168.254.3 0
rule 1000 deny ip
#
interface Aux0
async mode flow
#
interface Ethernet0/0
shutdown
#
interface Ethernet0/1
shutdown
#
interface Ethernet0/2
speed 100
duplex full
description to server
ip address 192.168.254.1 255.255.255.248
firewall packet-filter 3002 inbound

firewall aspf 1 outbound
#
interface Ethernet0/3
shutdown
#
interface Ethernet1/0
shutdown
#
interface Ethernet1/1
shutdown
#
interface Ethernet1/2
speed 100
duplex full
description to internet
ip address 202.111.0.1 255.255.255.224
firewall packet-filter 3001 inbound
firewall aspf 1 outbound
nat outbound static
#
interface NULL0
#
firewall zone local
set priority 100
#
firewall zone trust
add interface Ethernet0/2
set priority 85
#
firewall zone untrust
add interface Ethernet1/2
set priority 5
#
firewall zone DMZ
add interface Ethernet0/3

set priority 50
#
firewall interzone local trust
#
firewall interzone local untrust
#
firewall interzone local DMZ
#
firewall interzone trust untrust
#
firewall interzone trust DMZ
#
firewall interzone DMZ untrust
#
ip route-static 0.0.0.0 0.0.0.0 202.111.0.30 preference 60
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
authentication-mode scheme
#

APPENDIX 2

SWITCH SECURITY CONFIGURATION COMMANDS

3550-1#conf t
3550-1(config)#int f0/1
3550-1(config-if)#switchport mode access
3550-1(config-if)#switchport port-security mac-address 00-90-F5-10-79-C1
3550-1(config-if)#switchport port-security maximum 1

3550-1(config-if)#switchport port-security violation shutdown

3550-1(config)#int f0/1
3550-1(config-if)#switchport trunk encapsulation dot1q
3550-1(config-if)#switchport mode trunk
3550-1(config-if)#switchport port-security maximum 100
3550-1(config-if)#switchport port-security violation protect

APPENDIX 3

Enable vpn server

l2tp enable

domain system

ip pool 1 192.168.254.5 192.168.254.100

#

local-user guest

passwored simple guest

servicce-type ppp

#

interface virtual-template1

ppp authentication-mode pap

ip 192.168.254.1 255.255.255.0

remote address pool 1

#

l2tp-group 1

allow l2tp vistual-template 1 remote client

tunnel password simple 123

tunnel name client

#

ip rout-static 192.168.254.0 255.255.255.0 vritual-template 1 preference 60

Enable vpn client

l2tp enable

#

local-user guest

password simple guest

service-type ppp

```
#
interface virtual-template1
ppp authentication-mode pap
ppp pap local-user guest password simple guest
l2tp-quto-client enable
ip add ppp-negotiate
#
l2tp-group 1
tunnel password simple 123
tunnel name client
start l2tp ip 58.61.143.2 fullusername guest
```